

1/5/3 (Item 3 from file: 351)  
DIALOG(R) File 351: Derwent WPI  
(c) 2004 Thomson Derwent. All rts. reserv.

012306767 \*\*Image available\*\*  
WPI Acc No: 1999-112873/ 199910  
XRPX Acc No: N99-082744

Calling party authentication method in communication network e.g. for PHS  
- involves authenticating information terminal equipment to be contract  
user of calling party based on calling party telephone number, password  
and user account number of terminal equipment

Patent Assignee: SONY CORP (SONY )  
Number of Countries: 001 Number of Patents: 001  
Patent Family:

| Patent No   | Kind | Date     | Applicat No | Kind | Date     | Week     |
|-------------|------|----------|-------------|------|----------|----------|
| JP 10336345 | A    | 19981218 | JP 97146981 | A    | 19970605 | 199910 B |

Priority Applications (No Type Date): JP 97146981 A 19970605

Patent Details:  
Patent No Kind Lan Pg Main IPC Filing Notes  
JP 10336345 A 7 H04M-011/00

Abstract (Basic): JP 10336345 A.

NOVELTY - A calling party registers a communication access demand based on the telephone number of an information terminal equipment. A logic path is formed between the calling party and the terminal equipment, when the terminal equipment is authenticated to be the contract user corresponding to the telephone number. The authentication is confirmed based on the password and the user account number of the terminal equipment.

USE - For PHS.

ADVANTAGE - The authentication security level in the calling party authentication is improved.

Dwg.1/5

Title Terms: CALL; PARTY; AUTHENTICITY; METHOD; COMMUNICATE; NETWORK;  
AUTHENTICITY; INFORMATION; TERMINAL; EQUIPMENT; CONTRACT; USER; CALL;  
PARTY; BASED; CALL; PARTY; TELEPHONE; NUMBER; PASSWORD; USER; ACCOUNT;  
NUMBER; TERMINAL; EQUIPMENT

Derwent Class: W01; W02

International Patent Class (Main): H04M-011/00

International Patent Class (Additional): H04M-001/57; H04M-001/66

File Segment: EPI

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-336345

(43) 公開日 平成10年(1998)12月18日

(51) Int.Cl.<sup>8</sup>

H 0 4 M 11/00  
1/57  
1/66

識別記号

3 0 3

F I

H 0 4 M 11/00  
1/57  
1/66

3 0 3

B

審査請求 未請求 請求項の数10 O L (全 7 頁)

(21) 出願番号 特願平9-146981

(22) 出願日 平成9年(1997)6月5日

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 川本 洋志

東京都品川区北品川6丁目7番35号 ソニー株式会社内

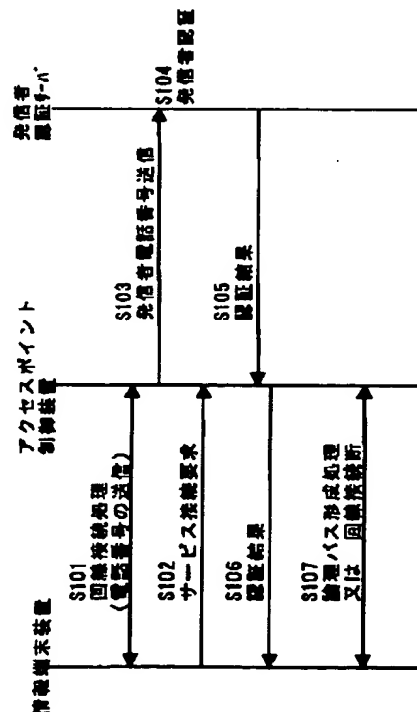
(74) 代理人 弁理士 松原 伸之 (外2名)

(54) 【発明の名称】 通信ネットワーク・システムにおける発信者認証方法、情報端末装置及び情報提供装置

(57) 【要約】

【課題】 個人使用の情報処理装置からのインターネット等の通信システムに対する通信回路接続要求の際に行われる発信者認証手続きにおいて、セキュリティ・レベルの高い認証方法を提供する。

【解決手段】 従来のアカウントコードとパスワードによる発信者認証方法に代えて、通信ネットワークに接続された情報提供装置に対してアクセスポイントを介してアクセス要求する情報端末装置を、前記情報提供装置は、前記情報端末装置の発信者電話番号に基づいて該発信者が登録されている契約ユーザであることを認証し、それにより前記情報端末装置との論理パスを形成することとする。これにより契約に係る情報端末装置そのものを該情報端末装置が有する電話手段の固有の電話番号に基づいて認証することから、発信者認証における認証セキュリティ・レベルが向上すると共に、通信アクセスの際における操作の簡易化を実現した。



## 【特許請求の範囲】

【請求項 1】通信ネットワークに接続された情報提供装置に対してアクセスポイントを介してアクセス要求する情報端末装置の発信者認証方法であって、

前記情報提供装置は、前記情報端末装置の発信者電話番号に基づいて該発信者が登録されている契約ユーザであることを認証し、それにより前記情報端末装置との論理パスを形成することを特徴とする通信ネットワーク・システムにおける発信者認証方法。

【請求項 2】前記情報提供装置は、前記発信者電話番号と共に当該情報端末装置から送信されるパスワードとユーザ・アカウント番号に基づいて該発信者が登録されている契約ユーザであることを認証することを特徴とする請求項 1 に記載の通信ネットワーク・システムにおける発信者認証方法。

【請求項 3】通信ネットワークに設けられたアクセスポイントを経由して情報提供装置にアクセス要求する情報端末装置の通信ネットワーク・システムにおける発信者認証方法であって、

前記情報端末装置は、前記アクセスポイントにおける制御装置を介して前記情報提供装置に対して回線接続を要求するステップと、

回線接続がなされた後、前記情報端末装置は、前記制御装置を経由して前記情報提供装置に対して自己の電話番号を送信するステップと、

前記情報提供装置は、受信した前記電話番号が予め登録されている契約ユーザの電話番号であるか否かを自己のデータ・ベースに基づいて認証するステップと、

前記情報提供装置は、該認証結果を前記制御装置に送信するステップと、

前記中継器は、前記認証結果を前記制御装置を介して前記情報端末装置に対して送信するステップと、

前記認証に基づいて、前記情報端末装置と前記情報提供装置間には論理パスが形成され、該情報提供装置は該情報端末装置からの所定の情報サービスの提供要求を受け入れるステップと、の各行程からなることを特徴とする通信ネットワーク・システムにおける発信者認証方法。

【請求項 4】前記電話番号を送信するステップは、前記制御装置が前記情報端末装置の電話番号を検出し、該検出した電話番号を前記情報提供装置に送信することを特徴とする請求項 3 に記載の通信ネットワーク・システムにおける発信者認証方法。

【請求項 5】前記電話番号を送信するステップは、電話番号と共に予め登録した自己のパスワードとユーザ・アカウント番号とを送信するステップであり、且つ前記認証するステップは、電話番号と共に前記パスワードによって当該情報端末装置を認証することを特徴とする請求項 3 に記載の通信ネットワーク・システムにおける発信者認証方法。

【請求項 6】通信ネットワークに設けられたアクセスポ

イントを経由して情報提供装置にアクセス要求する情報端末装置であって、

前記アクセスポイントに回線接続するための電話手段と、

回線接続後に、前記情報提供装置間と情報通信を行うための通信制御手段と、を有し、

前記通信制御手段は、前記情報提供装置に対して所定の情報サービスの提供を要求する際に、前記情報提供装置による発信者認証のために自己の電話番号を送信して前記情報提供装置との論理パスの形成を求めることを特徴とする情報端末装置。

【請求項 7】前記情報端末装置は、PHS (Personal Handyphone System: 簡易型携帯電話) 機能を有することを特徴とする請求項 6 に記載の情報端末装置。

【請求項 8】前記通信制御手段は、前記電話番号のほかに、前記情報提供装置に対して予め登録してあるパスワードとユーザ・アカウント番号を送信することを特徴とする請求項 6 に記載の情報端末装置。

【請求項 9】アクセスポイントを介して通信ネットワークに接続される電話手段を有する情報端末装置に対して、種々の情報サービスの提供を行う情報提供装置であって、

前記アクセスポイントを介して前記情報端末装置間と情報通信を行うための通信制御手段と、

前記情報サービスの提供を行う契約ユーザの前記情報端末装置の電話番号リストを記憶する記憶手段と、

前記情報端末装置から所定の情報サービスの提供要求を受ける際に、当該情報端末装置から送信された電話番号が前記記憶手段に記憶されている電話番号リスト内の一つであることを認証する認証手段と、を有し、

前記認証によって、当該情報端末装置との論理パスを形成し前記所定の情報サービスの提供要求を受け入れることを特徴とする情報提供装置。

【請求項 10】前記記憶装置には、前記電話番号と共に、契約者が予め選定したパスワードとユーザ・アカウント番号が記憶され、前記認証手段は、情報サービスの提供を要求する情報端末装置の認証を、電話番号、パスワード及びユーザ・アカウント番号によって行うことを特徴とする請求項 9 に記載の情報提供装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

【0002】本発明は、通信ネットワークに接続された情報提供装置に対して情報サービスの提供を要求する通信ネットワーク・システムにおける情報端末装置の発信者認証方法、情報端末装置及び情報提供装置に関する。特に、PHS (Personal Handyphone System: 簡易型携帯電話) 等のパーソナル・デジタル無線通信機能を有する情報端末装置に対する情報提供装置による発信者認証方法等に関する。

【従来の技術】インターネット等の情報通信ネットワーク（以下、単に「通信ネットワーク」という）の発展により、通信ネットワークにアクセス可能な通信機能を有するパーソナル・コンピュータ等の情報処理装置（以下、「情報端末装置」という）の利用が増大している。

【0003】情報端末装置を通信ネットワークに接続して所定の情報サービスの提供を受けようとする場合、通常、該通信ネットワークへの回線接続サービスを提供する商用プロバイダ（以下、単に「プロバイダ」という）と前もって契約を取り交わす必要がある。このような契約を取り交わした情報端末装置のユーザは、情報サービスの提供を受けようとする際、プロバイダが提供するアクセスポイント（回線接続用電話番号）の一つにダイヤルアップ接続を行い、当該アクセスポイントを介してその通信ネットワークに接続されている通常サーバと呼ばれる情報提供装置への通信リンクの確立を要求することとなる。そして、プロバイダの発信者認証用の情報提供装置は、当該情報端末装置のユーザが契約者の一人であることを認証した上で、当該情報端末装置との論理パスを形成し、所定の情報サービスの提供を行うこととなるのである。

【0004】このように、プロバイダが設置する発信者認証用の情報提供装置により認証され、通信ネットワークとの論理パスが形成された情報端末装置のユーザは、通信ネットワークに接続されている各種サーバ、例えばWWW（World Wide Web）サーバが提供する情報の検索と取得、ニュース・サーバから種々の情報の入手、電子メール・サーバを介して他の情報端末装置間と電子メールの通信等の情報サービスの提供を受けることができるのである。

【0005】図5に示すとおり、情報提供サービスを受ける際の従来における上記発信者認証手続きは、情報端末装置が、所定のアクセスポイントにダイヤルアップ接続を行った後に、当該ユーザがプロバイダとの契約時に定めた自己のアカウントコードとパスワードを送信し、それをプロバイダの発信者認証用情報提供装置が登録されている契約者のものであることを確認することにより行われていた。この場合、情報提供装置による前記確認結果は、当該アクセスポイントにおける制御装置に通知され、それを受けて制御装置は、当該アクセスが契約者によるものであれば通信ネットワークとの論理パスを形成させ、契約者によるものでなければその旨を通知した上で、該ダイヤルアップ接続処理を中断させるようにしていたのである。

【0006】

【発明が解決しようとする課題】しかし、このようなアカウントコードとパスワードによる発信者認証方法は、通信アクセスを要求してきた情報端末装置そのものを物理的に確認し認証するものではないことから、発信者認証のセキュリティ・レベルとしては低いものであると言

わざるを得ない。つまり、当該アカウントコードとパスワードを知るに至った契約者以外の者による通信アクセスの要求に対しても、これらのコードが、登録されている契約者のものであれば、情報提供装置は、当該情報端末装置からの通信アクセス要求を受け入れてそれとの論理パスを形成をすることとなり、該情報端末装置の要求に応じて情報サービスを提供し、当該情報サービスの提供に係る費用請求は当該コードの契約者に対して行われることとなるのである。

10 【0007】また、通信ネットワークにアクセスする度に自己のアカウントコードとパスワードを送信しなければならないため、通信アクセスの際の操作が煩雑であり、特に、手のひら上で操作するPHS等のパーソナル・デジタル無線通信機能を有するPDA（Personal Digital Assistants:個人用携帯情報装置）等の携帯端末装置の場合に操作性上の問題があった。

【0008】

【課題を解決するための手段】このため、本願発明においては、従来のアカウントコードとパスワードによる発信者認証方法に代えて、通信ネットワークに接続された情報提供装置に対してアクセスポイントを介してアクセス要求する情報端末装置の発信者電話番号に基づいて、情報提供装置が該発信者が登録されている契約ユーザであることを認証し、それにより前記情報端末装置との論理パスを形成することとした。これにより契約に係る情報端末装置そのものを該情報端末装置が有する電話手段の固有の電話番号に基づいて認証することから、発信者認証における認証セキュリティ・レベルが向上すると共に、通信アクセスの際における操作が簡易化されることとなるのである。

【0009】

【作用】このように、本願発明においては、通信ネットワークへの通信アクセスを要求する発信者の認証を、情報端末装置と共に用いられる現実の電話手段の電話番号に基づいて行うこととしている。これにより、パーソナル・ユースの情報端末装置、特にPDA等の携帯用情報端末装置のように一個人が物理的に占有した状態で使用するような場合における、発信者認証のセキュリティ・レベルを大きく向上することができるのである。

40 【0010】

【発明の実施の形態】以下、本願発明に係る発信者認証方法、情報端末装置及び発信者認証用の情報提供装置について、図面に基づいて詳しく説明する。

【0011】図1は、情報端末装置が接続される公衆通信網、インターネットを含む通信ネットワーク・システムの全体概要の例を示す。

50 【0012】情報端末装置1は、それぞれが電話手段及び通信制御手段を有するパーソナル・コンピュータ1-1、1-2若しくはPDA1-3等の情報処理装置である。PDA1-3は、PHS等のパーソナル・ディジタ

## 5

ル無線通信手段を有し、それによって通信ネットワークにアクセスすることができる。PDA 1-3 が PHS 通信手段を使って通信ネットワークにアクセスする際には、当該 PHS 電話システムを運営する通信事業者が提供する無線通信ネットワークを構成する基地局 11のうち、最寄りの基地局と電波によって通信することができる。情報端末装置 1 を接続する公衆通信網 2 は、プロバイダ 3 が所有するプロバイダ通信網 4 を介してインターネット 7 と接続されている。

【0013】情報端末装置 1 のユーザは、通信ネットワークに接続して種々の情報サービスの提供を受けようとする場合、通信ネットワークへの回線接続サービスを提供するプロバイダ 3 と契約を締結した上で該プロバイダ 3 が公衆回線上に設置するアクセスポイント 10 に電話接続する。各アクセスポイントにおける制御装置は、通信アクセスを要求してきた当該情報端末装置 1 のユーザが契約者であることの確認手続（認証）を取ったうえで、その情報端末装置の通信ネットワークへの通信アクセスを認める論理パスを形成することとなるのである。

【0014】こうして通信ネットワークにアクセスできた情報端末装置 1 は、プロバイダ通信網 4 に接続されている各種サーバ 6 が提供する種々の情報サービスを受けることができるのである。例えば、メール・サーバ 6c を介した情報端末装置 1 相互間の電子メールによる情報の交換、ニュース・サーバ 6d からの最新ニュース情報の取得等の情報サービスである。さらに、通信ネットワークにアクセスを許された情報端末装置 1 は、プロバイダ通信網 4 からインターネットへの接続装置であるゲートウェイ 5 を経由してインターネット 7 上の特定の WWWサーバ 8i から情報を得ることができる。インターネットに接続されている特定の WWWサーバ 8i にアクセスするには、通常 TCP/IP と呼ばれる通信プロトコルに従い、WWWブラウザと呼ばれる WWWサーバへの情報検索用アプリケーション・ソフトウェアを使用して、アクセス先アドレスとして直接 URL (Uniform Resource Locator) を入力すればよい。URL は、WWWサーバ 8i のアドレスを http://ホスト名.ドメイン名/ファイル名の形式で示している。URL が入力されると、サーバの一つである DNS (Domain Name System) サーバ 6a が、自己のデータ・ベースを参照して、当該 URL に対応する現実のインターネット上のアドレスである TCP/IP アドレスを見出し、ゲートウェイ 5 を介してその情報端末装置 1 を目的とする WWWサーバ 8i に接続するのである。このようにして、情報端末装置 1 と WWWサーバ 8i との接続が確立されると、WWWブラウザは、その WWWサーバ 8i 内にあるファイルを検索し、HTTP (Hyper Text Transfer Protocol) の通信プロトコルに基づいて当該ファイルを自己の情報端末装置 1 に読み込むことができるのである。

【0015】図 2 は、本発明に係る情報端末装置の内部

## 6

構成の一例を示す。図 2 において、CPU (Central Processing Unit: 中央演算処理装置) 12 は、メモリ装置に格納されているプログラムに従って各種のデータ情報処理を行う本装置の中枢部である。メモリ装置は、その性質によって、ROM (Read Only Memory : 読出し専用メモリ) 13 と、RAM (Random Access Memory : 随時書き込み読み出しメモリ) 14 に分類される。ROM 13 には、主に固定データやプログラムが格納され、RAM 14 には、変動データや他の記憶装置、ディスク装置等から適宜読み出されたデータやプログラムが格納される。尚、RAM 14 には、通信ネットワークに対して通信アクセスする際に必要な、電話番号若しくはアカウントコード等を予め格納することにより、入力部 23 の所定キーによるクリック等によるとり簡便なダイアルアップ操作を可能とする。

【0016】入力部 23 は、キー、ボタン、スイッチ等により構成され、これにより情報端末装置に所定の情報入力及び情報処理の指示を与える。音声出力部 20 は、スピーカと増幅器を有し、入力操作を補助するための信号音や、外部からの音声データを再生するためのものである。表示部 21 は、画像や文字情報を視覚的に表示するためのものであり、情報端末装置 1 がデスクトップ型であれば、CRT 等、携帯型や PDA 1-3 の場合であれば、LCD (Liquid Crystal Display : 液晶表示装置) などの電力消費の少ない表示装置によって構成される。

【0017】HDD (Hard Disc Drive) 装置 22 は、プログラムや画像データ等の大容量のデータを磁気的に記憶しておくための装置であり、データは RAM 14 に適宜転送されて利用される。HDD 装置 22 は、サイズ及び重量等の関係で PDA 1-3 には搭載されないことが多いが、用途によっては、携帯型情報端末装置にも搭載されるようになってきている。電話/通信制御部 24 は、モデム等の電話通信手段及び送信手段と受信手段からなり、通信ネットワークとの通信制御を司る。PHS を搭載する PDA の場合は、アンテナ手段 25 を有し、最寄りの基地局 11 と通信リンクを形成し無線によって通信が行えるように構成されている。

【0018】音声出力部 20、表示部 21、HDD 装置 22、入力部 23 及び電話/通信制御部 24 は、それぞれの入出力信号をバス（アドレスバスとデータバス）15 に接続するためのインターフェース 16 を有する。

【0019】図 3 は、通信アクセスを要求する情報端末装置 1 に対し、発信者認証を行うための情報提供装置 6a の内部構成例を示す。

【0020】この情報提供装置 6a は、プロバイダ通信網に接続され、各アクセスポイントにおける制御装置からの発信者認証に関する問い合わせに対して、認証確認業務を担当するサーバである。

【0021】CPU 32、ROM 33 及び RAM 34 の

働きは、情報端末装置 1 における上述した説明と同様である。情報提供装置 6 a における HDD 装置 4 3 には、当該プロバイダとの登録契約ユーザの一覧データがデータベースの形式で格納されている。該一覧データは、少なくとも全登録契約ユーザの個々のアカウントコード、パスワードそして電話番号情報を含み、これらのコード等の任意の一つ若しくは複数の組み合わせに関する問い合わせに対して、登録契約ユーザのものであるか否かを短時間で検索可能なデータベースの形式で構成されている。

【0022】通信制御部 4 0 は、プロバイダ通信網 4 に直接に接続され、ISDN 等の公衆回線を経由して各アクセスポイントの制御装置と送受信するための通信制御機能を有する。

【0023】入力部 4 2 は、キーボード及びマウス等により構成され、当情報提供装置 6 に所定の情報処理を行わせるための指令やデータを入力するためのものである。新規加入契約者の関連データは、入力部 4 2 の操作を介して HDD 装置 4 3 にインプットされる。表示部 4 6 は、CRT 又は LCD 等により構成され、文字及び画像情報を表示するを表示する。

【0024】通信制御部 4 0、表示部 4 1、入力部 4 2 及び HDD 装置 4 3 は、それぞれの入出力信号をバス（アドレスバスとデータバス）3 5 に接続するためのインターフェイス 3 6 を有する。

【0025】図 4 は、通信アクセスを要求する情報端末装置の本発明に係る発信者認証手続シーケンス例を示す。

【0026】前記したように、従来技術においては図 5 に示すように、情報端末装置 1 のユーザが通信ネットワークにアクセスして、情報の交換、検索若しくは取得等の情報サービスの提供を受ける際には、プロバイダによって当該ユーザが登録された契約者の一人であることの認証手続きを必要とする。そして、従来におけるこの発信者認証手続きは、情報端末装置が、所定のアクセスポイントにダイヤルアップ接続を行った後に、当該ユーザがプロバイダとの契約時に定めた自己のアカウントコードとパスワードを送信し、それをプロバイダが設けたサーバの一つである発信者認証用情報提供装置が登録されている契約者のものであることを確認することにより行われていたである。

【0027】これに対して本発明においては、図 4 に示すように、通信ネットワークから所定の情報サービスの提供を受けようとする情報端末装置 1 のユーザは、情報端末装置 1 を起動した後に、先ずプロバイダが設置している最寄りのアクセスポイント 1 0 の電話番号に電話発呼することによりプロバイダ 3 に対して通信ネットワークへの通信アクセスを要求する（S 1 0 1）。情報端末装置 1 は、この時必要に応じて自己の情報端末装置が搭載する電話手段の電話番号を送信する。そして、情報端

末装置 1 のユーザは、その後所定の情報サービスを受けるための接続要求信号を送出する（S 1 0 2）。

【0028】プロバイダ 3 の前記アクセスポイントにおける制御装置 1 0 は、この電話発呼を受け付け、情報端末装置 1 が通信ネットワークへの通信アクセス要求を確認したならば、発信者認証用の情報提供装置 6 a に対して、該情報端末装置 1 に搭載されている電話手段の電話番号を送信する（S 1 0 3）。前記手続の S 1 0 1 において情報端末装置 1 から送信されてきた電話番号が、前記制御装置が回線接続中に自動検出した発信者電話番号と相違する場合は、自動検出した番号を送出するようにする。これによってプロバイダ側は、当該情報端末装置 1 から送信された発信者電話番号が、当該情報端末装置が有する電話手段のものと同一であるか否かの物理的認証を取ることができるのである。アクセスポイントにおける制御装置は、送信されてきた電話番号が誤りであったならば、それを該情報端末装置ユーザの入力ミスとして、その番号を自動検出した電話番号に代えて発信者認証サーバ 6 a に送信する。これにより、発信者電話番号と該情報端末装置が搭載する電話手段の現実の電話番号との同一性を維持するのである。

【0029】このようにしてアクセスポイントにおける制御装置からプロバイダの発信者認証用の情報提供装置 6 a に送信されたユーザの電話番号は、情報提供装置 6 a に接続された HDD 装置 4 3 内のデータベースを検索して、それが登録契約ユーザの電話番号であるか否か認証する（S 1 0 4）。そしてその認証結果は、情報提供装置 6 a からアクセスポイントにおける制御装置 1 0 に送信され（S 1 0 5）、該制御装置 1 0 は、同認証結果を通信アクセスを要求した情報端末装置 1 に送信する（S 1 0 6）。

【0030】前記認証結果が、登録契約ユーザによるものであるとの認証であるならば、制御装置は、当該情報端末装置と通信ネットワークとの論理バスを形成させて、該情報端末装置からの所定の情報サービスの提供要求を受け入れる（S 1 0 7）。ところが、前記認証結果が、登録契約ユーザ以外からのものであった場合には、前記制御装置 6 a は、当該情報端末装置に対しその旨を送信するとともに回線接続を断つようにする。

【0031】本願発明においては、このように、通信ネットワークへの通信アクセスを要求する発信者の認証を、当該ユーザが物理的に占有使用する情報端末装置の電話手段の電話番号に基づく物理的認証によって行っているが、発信者認証におけるセキュリティ・レベルをより高める必要がある場合には、当然のことながら、電話番号とともに当該ユーザのアカウント・コードとパスワードの併用が可能である。

【0032】

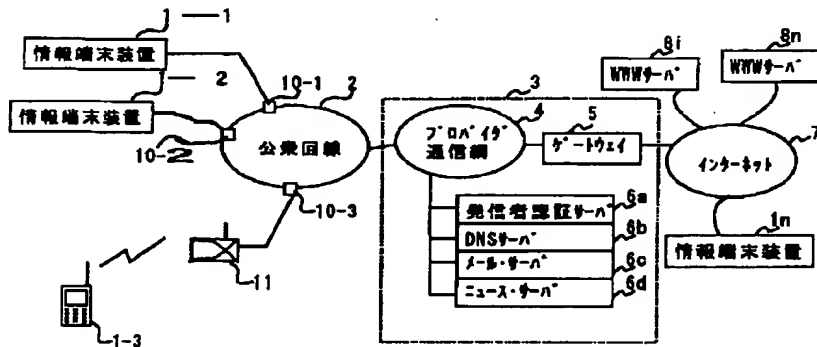
【発明の効果】以上説明したように、本願発明においては、通信ネットワークへの通信アクセスを要求する発信

者の認証を、該情報端末装置の電話手段の固有の電話番号に基づいて行うこととしている。これにより、パーソナル・ユースの情報端末装置、特にPDA等の携帯用情報端末装置のように一個人が物理的に占有した状態で使用するような場合に、発信者認証手続における認証セキュリティ・レベルを大きく向上することができ、さらに、通信アクセスの際における情報端末装置の操作の簡便化を実現し、ユーザは通信システムにアクセスする際、特に認証手続きを意識しなくとも、情報の検索、取得若しくは電子メール等の情報サービスの提供を受けることを可能にしたのである。

【図面の簡単な説明】

【図1】情報端末装置が接続される公衆通信網、インターネットを含む通信ネットワーク・システムの全体概要の例を示す。

【図1】



【図2】本発明に係る情報端末装置の内部構成例を示す。

【図3】発信者認証用の情報提供装置6aの内部構成例を示す。

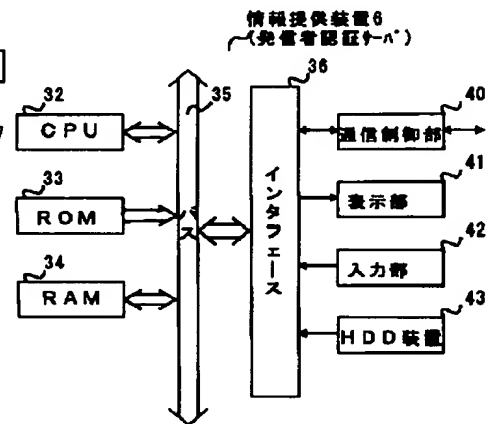
【図4】本発明に係る、通信アクセスを要求する情報端末装置の発信者認証手続シーケンス例を示す。

【図5】従来技術に係る、通信アクセスを要求する情報端末装置の発信者認証手続シーケンスを示す。

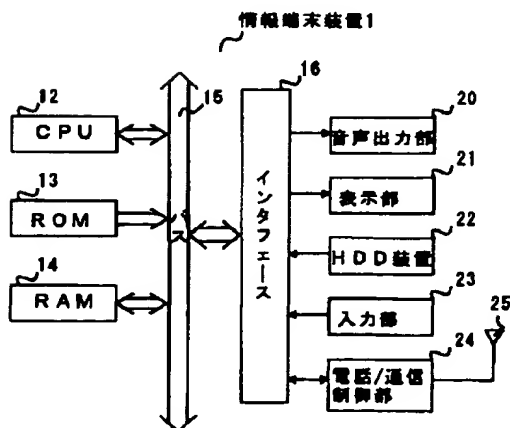
【符号の説明】

- 1-1、1-2：電話通信機能を有する情報端末装置
- 1-3：PHS等の無線通信手段を有する携帯用情報端末装置
- 10-n：アクセスポイントにおける制御装置
- 11：PHS等の無線受信基地局

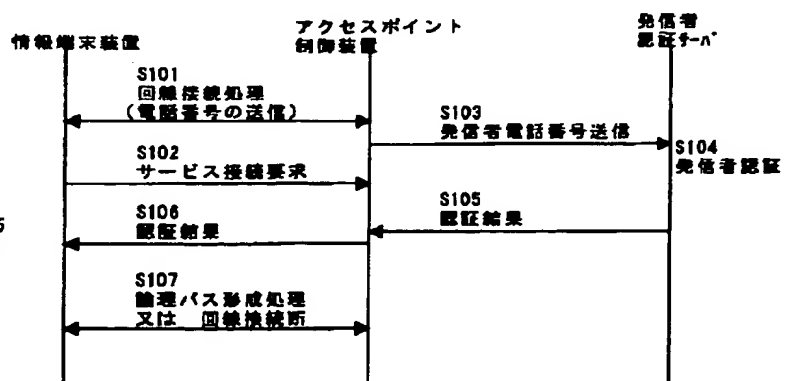
【図3】



【図2】



【図4】



【図 5】

